JOURNAL OF ALGEBRA **146**, 441–453 (1992)

# Maximal Orders in Nonassociative Quaternion Algebras*

HEE JUNG LEE

*Department of Mathematics, Ewha Women's University, Seoul, Korea*

AND

WILLIAM C. WATERHOUSE

*Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802*

*Communicated by Susan Montgomery*

Received March 7, 1990

## INTRODUCTION

Let $K$ be a field, and let $E$ be a separable quadratic extension of $K$, with $K$-conjugation $x \mapsto \bar{x}$. Let $A$ be a four-dimensional algebra over $K$ of the form $E \oplus EJ$ where $Jx = \bar{x}J$ for $x$ in $E$. Let $J^2 = b$. If $b$ were in $K$, we would have one of the usual quaternion algebras. In this paper we take the same definition but with $b$ in $E$ outside $K$. Our $A$ then is still a division algebra, though it is nonassociative, and we call it a *nonassociative quaternion algebra*. Products involving a factor from $E$ still satisfy associativity, and indeed this fact can be used to characterize such algebras abstractly [7]. They have been familiar examples of nonassociative division algebras for over half a century [2].

Now let $R$ be a Dedekind domain with fraction field $K$. As in the associative case, we can define an *($R$-)order* in $A$ to be an $R$-submodule $M$ of $A$ containing 1, having rank 4, and closed under multiplication. No one previously seems to have realized that the maximal orders in these algebras might have interesting properties. The corresponding question in ordinary quaternion algebras has been extensively studied [4, 6], but the theory here turns out to be quite different. In Section 3 we shall classify the isomorphism classes of maximal orders containing $S$, the integral closure of

* This work was supported in part by the U. S. National Science Foundation, Grant DMS8701690. Some of the results appeared in the doctoral dissertation by Lee at the Pennsylvania State University, 1989.



0021-8693/92 $3.00

$R$ in $E$; when $R=\mathbb{Z}$, for instance, there will usually be one such class for every element of the principal genus in the strict ideal class group of $S$. In Section 4, we shall then prove that in most cases every maximal order does in fact contain $S$. This proof will depend on the complete determination of maximal orders established by Lee [3] for the "split" versions of our algebras. In Section 5, finally, we shall use that same determination to show that in exceptional cases there can indeed be maximal orders not containing $S$.

## 1. Basic Properties of the Algebras and Orders

Without loss of generality we can replace $J$ by $sJ$ for $s$ in $E$, and this will replace $b=J^2$ by $s\bar{s}b$. By suitable choice of $s$, then, we can and do

*assume that $b$ is in $S$.*

Now we recall [7] the automorphisms of the algebra $A$; there are not so many of them as in the associative case. Specifically, the mappings of the form $\varphi(x+yJ)=x+\gamma yJ$ with $N_{E/K}(\gamma)=1$ are automorphisms. They are the only ones unless $b/\bar{b}=-1$ and there are elements $\gamma$ in $E$ with $N_{E/K}(\gamma)=-1$; in that case the maps of the form $\varphi(x+yJ)=\bar{x}+\gamma\bar{y}J$ are also automorphisms. Clearly all automorphisms of $A$ send the field $E$ to itself. The automorphisms of the first type, trivial on $E$, will be called *proper* automorphisms.

Proposition 1.1. *Let $N$ and $N_1$ be orders in $A$. If they are isomorphic, then $N\cap E=N_1\cap E$.*

*Proof.* Any $R$-isomorphism from $N$ to $N_1$ will extend to a $K$-automorphism $\varphi$ of $A$. The result then is trivial if $\varphi$ is proper. For improper $\varphi$, we observe that $N\cap E$ is a subring of $E$ finitely generated as a module over $R$, so it is contained in the integral closure $S$ of $R$ in $E$. For $x$ in $N\cap E$ then we have $\varphi(x)=\bar{x}=(x+\bar{x})-x=\mathrm{Tr}_{E/K}(x)-x$ again lying in $N\cap E$. ∎

Corollary 1.2. *The set of orders in $A$ containing $S$ is closed under isomorphism.*

This is not true for ordinary quaternions.

Right multiplication by an element $x+yJ$ in $A$ is an $E$-linear mapping of $A$ to $A$, and its characteristic polynomial comes out to be $\lambda^2-(x+\bar{x})\lambda+x\bar{x}-by\bar{y}$. As a $K$-linear mapping, the right multiplication has characteristic polynomial

$$\{\lambda^2-(x+\bar{x})\lambda+x\bar{x}-by\bar{y}\}\cdot\{\lambda^2-(x+\bar{x})\lambda+x\bar{x}-\bar{b}y\bar{y}\}.$$

(In the associative case, this polynomial would be a square; here it is not, but at least it still factors into two quadratics.) It is easy to check that left multiplication by $x + yJ$ has this same characteristic polynomial over $K$. We can eliminate a factor of 2 in the trace if we define the *reduced trace* of $x + yJ$ to be

$$\mathrm{tr}(x + yJ) = \mathrm{Tr}_{E/K}(x) = x + \bar{x}.$$

The reasoning in Proposition 1.1 shows that this is an intrinsic invariant, unchanged by automorphisms of $A$.

PROPOSITION 1.3. *Let $N$ be an order in $A$. Then $\mathrm{tr}(x + yJ)$ is in $R$ for all $x + yJ$ in $N$.*

*Proof.* Right multiplication by $x + yJ$ has a characteristic polynomial with coefficients in $R$, as it maps the finitely generated $R$-module $N$ to itself. As $R$ is integrally closed, it follows [1, p. 17] that the factors of this monic polynomial have coefficients in $R$. ∎

If $a_1, ..., a_4$ is a $K$-basis of $A$, we define its discriminant to be $\det(\mathrm{tr}(a_i a_j))$. In the basis 1, $b$, $J$, $bJ$, the discriminant is $-b\bar{b}[2 \cdot \mathrm{tr}(b^2) - (\mathrm{tr}(b))^2]^2$, which is easily seen to be nonzero; hence the discriminant of any basis is nonzero. We define the *discriminant of an order $N$* in $A$ to be the ideal of $R$ generated by discriminants of all bases contained in $N$.

PROPOSITION 1.4. *If we have a proper inclusion $N \subset N_1$ of orders in $A$, then the discriminant of $N$ is a nontrivial square factor times the discriminant of $N_1$.*

*Proof.* Though the bilinear form $\mathrm{tr}(cd)$ is not symmetric in our situation, the general reasoning about discriminants [4, p. 66] still remains valid. ∎

COROLLARY 1.5. *Maximal orders exist in $A$, and every order in $A$ is contained in a maximal order.*

*Proof.* The second statement is clear from (1.4), and thus we just need to show an order exists. As we have $b$ in $S$, we can take the submodule $S \oplus SJ$. ∎

## 2. MAXIMAL ORDERS CONTAINING $S$: THE LOCAL CASE

In this section we assume that $R$ is a discrete valuation ring. There are three possibilities for $S$: either the prime of $R$ stays prime, or it splits into

two primes, or it ramifies. The first two of these cases will be easy to analyze, but the third will require some work and will depend on the precise nature of the element $b$. Recall that $\{v \in E \mid \mathrm{Tr}_{E/K}(vS) \subseteq S\}$ is a fractional ideal of $S$ whose inverse is called the different; it equals $S$ unless the prime ramifies.

LEMMA 2.1. *If $N$ is an order containing $S$, then $N = S \oplus S(u + vJ)$ for some $u + vJ$ in $A$.*

*Proof.* Clearly $N$ is a torsion-free left $S$-module of rank 2; and hence it is free of rank 2, since $S$ is semi-local. As in (1.1), we have $E \cap N = S$, so $S$ is a direct summand. ∎

LEMMA 2.2. *Suppose $S \oplus S(v + wJ)$ is an order. Then $v$ is in the inverse different of $S$ over $R$.*

*Proof.* For every $s$ in $S$, the order contains $(v + wJ)\, s(v + wJ) = \bar{s}(w\bar{w}b - v\bar{v}) + \mathrm{Tr}_{E/K}(vs)[v + wJ]$. Thus $\mathrm{Tr}_{E/K}(vS) \subseteq S$. ∎

PROPOSITION 2.3. *Suppose the prime $\pi R$ of $R$ stays prime in $S$. Then there is exactly one maximal $R$-order in $A$ containing $S$. Explicitly, it is $M = S \oplus \pi^{-m} SJ$, where $m = [(\mathrm{ord}_\pi b)/2]$.*

*Proof.* For any order $N = S \oplus S(v + wJ)$, Lemma 2.2 shows that $v$ is in $S$, and hence we may assume $v = 0$. The first term in the formula of 2.2 shows then that $w\bar{w}b$ is also in $S$. Hence we have $\mathrm{ord}_\pi w = \mathrm{ord}_\pi \bar{w} \geqslant -m$, and thus $N \subset M$. It is trivial to verify that $M$ is indeed an order. ∎

PROPOSITION 2.4. *Suppose the prime of $R$ splits as $\pi\bar{\pi}$ in $S$. Then there are countably many distinct maximal $R$-orders in $A$ containing $S$. Explicitly, they are $S \oplus S(\bar{\pi}/\pi)^n \pi^{-m} J$ for arbitrary integers $n$ and $m = \min(\mathrm{ord}_\pi b, \mathrm{ord}_{\bar{\pi}} b)$.*

*Proof.* As in (2.3), we can write any $N$ as $S \oplus SwJ$. We also must have $w\bar{w}b$ in $S$; that is, we have both $\mathrm{ord}_\pi(w\bar{w}b)$ and $\mathrm{ord}_{\bar{\pi}}(w\bar{w}b)$ non-negative. If we write $\mathrm{ord}_\pi w = c$ and $\mathrm{ord}_{\bar{\pi}}(w) = \mathrm{ord}_\pi(\bar{w}) = n$, then these conditions are easily seen to be equivalent to $c + n + m \geqslant 0$. Then $N = S \oplus S\pi^{c+n+m}(\bar{\pi}/\pi)^n \pi^{-m}$ is contained in one of the modules listed. It is trivial to verify that they are indeed orders and that no one of them is contained in another one. ∎

We now turn to the case where the prime of $R$ is ramified in $S$. Let $\pi S$ be the prime ideal in $S$. We recall some information about ramified quadratic extensions from [5, pp. 91–93]; the completeness assumed in some of the theorems there does not enter into any of the congruence results we need. Let $t$ be defined by $t + 1 = \mathrm{ord}_\pi(\bar{\pi} - \pi)$. This $t$ does not depend on the

choice of the uniformizer $\pi$, and the different of $S$ over $R$ is equal to $(\pi^{t+1})S$. We have $t=0$ iff the residue characteristic is not 2. Let $U_E^r = \{x \in S \mid x \equiv 1 \bmod \pi^r\}$, and let $U_K^r = \{x \in R \mid x \equiv 1 \bmod (\pi\bar{\pi})^r\}$. (For $r=0$, we take the groups of units.) The norm induces homomorphisms $U_E^r/U_E^{r+1} \to U_K^r/U_K^{r+1}$ for $0 \leqslant r \leqslant t$. These are one-to-one so long as $r < t$. When $r = t$, the kernel is cyclic of order two, and the nontrivial element in the kernel is given by the class of $\bar{\pi}/\pi$. It follows then easily that the norm induces a mapping from $U_E^0/U_E^s$ to $U_K^0/U_K^s$ which is injective for $s \leqslant t$ and has kernel of order 2 generated by the class of $\bar{\pi}/\pi$ when $s = t+1$.

PROPOSITION 2.5. *Suppose $S$ has the single ramified prime $\pi S$. Let $t+1 = \operatorname{ord}_\pi(\bar{\pi} - \pi)$, and let $k$ be the largest integer $\leqslant t+1$ such that there exists some $u$ in $E$ with $\operatorname{ord}_\pi(u\bar{u}b - 1) \geqslant 2k$. If $k$ is less than $t+1$, then there is just one maximal order containing $S$, namely $S \oplus S\pi^{-k}(1+uJ)$. If $k = t+1$, then there are exactly two maximal orders containing $S$, namely*

$$S \oplus S\pi^{-k}(1+uJ) \qquad \text{and} \quad S \oplus S\pi^{-k}(1+u(\bar{\pi}/\pi)J).$$

*Proof.* Suppose we have any order $N$ containing $S$. We know we can write it as $S \oplus S(v+wJ)$. Multiplying by a unit, we can assume by (2.2) that $v$ is $\pi^{-n}$ with $0 \leqslant n \leqslant t+1$. The computation in (2.2) shows also that the element $w\bar{w}b - (\pi\bar{\pi})^{-n}$ is in $S$. Writing $u = \pi^n w$, we have then $\operatorname{ord}_\pi(u\bar{u}b - 1) \geqslant 2n$. Hence $n \leqslant k$.

Suppose that we have two such orders with the same $n$, given by (say) $u$ and $u_1$. Let $u_1 = cu$. We have $u\bar{u}b \equiv 1 \equiv u_1\bar{u}_1 b \bmod \pi^{2n}$, and so $c\bar{c} \equiv 1 \bmod \pi^{2n}$. If $n \leqslant t$, then we know this condition on the norm implies that $c \equiv 1 \bmod \pi^n$. Hence we have

$$\pi^{-n}(1+u_1J) = \pi^{-n}(1+ucJ) = \pi^{-n}(1-c) + c\pi^{-n}(1+uJ),$$

and so $S \oplus S\pi^{-n}(1+u_1J) = S \oplus S\pi^{-n}(1+uJ)$. Thus there is actually only one such order. Furthermore, if we can find $u$ satisfying $\operatorname{ord}_\pi(u\bar{u}b - 1) \geqslant 2(n+1)$, then we obviously have

$$S \oplus S\pi^{-n}(1+uJ) \subset S \oplus S\pi^{-(n+1)}(1+uJ).$$

Hence the maximal orders are those occurring for $n = k$. When $k$ is less than $t+1$, then we have already seen that there is exactly one such maximal order. When $n = k = t+1$, we can repeat the argument to get $c\bar{c} \equiv 1 \bmod \pi^{2(t+1)}$, but now this gives the two possibilities $c \equiv 1 \bmod \pi^{(t+1)}$ and $c \equiv \bar{\pi}/\pi \bmod \pi^{(t+1)}$. ∎

THEOREM 2.6. *Let $R$ be local. Then the proper automorphisms $\varphi(x+yJ) = x + \gamma yJ$ with $N_{E/K}(\gamma) = 1$ act transitively on the set of maximal orders containing $S$. The stabilizer of any one order is*

(a) *all such* $\gamma$, *if the prime of* $R$ *is inert*;

(b) *those* $\gamma$ *that are units in* $S$, *if the prime of* $R$ *splits*;

(c) *those* $\gamma$ *congruent to* $1 \bmod \pi^k$, *if the prime of* $R$ *ramifies as* $(\pi^2)$ *and* $k$ *is the largest integer* $\leqslant \mathrm{ord}_\pi(\bar{\pi}-\pi)$ *for which there is some* $u$ *in* $E$ *with* $\mathrm{ord}_\pi(u\bar{u}b-1) \geqslant 2k$.

*Proof.* Clearly (2.3) gives us the inert case; and (2.4) gives us the split case, since $\bar{\pi}/\pi$ has norm 1. That same fact shows that the ramified case follows from (2.5). Observe that in the ramified case the stabilizer includes all $\gamma$ except when $k = t+1$. ∎

## 3. Maximal Orders Containing $S$: The Global Case

In this section, $R$ is again an arbitrary Dedekind domain, and $P$ will denote a prime ideal of $R$. We already know that maximal orders exist in our algebra $A$. We can use all the familiar local-to-global results on orders, as they do not require associativity. That is [5, p. 132], a finitely generated $R$-submodule $M$ of $A$ is an order (resp. a maximal order) iff each localization $M_P = M \otimes_R R_P$ is an order (resp. a maximal order) over $R_p$, and any two orders have the same localizations at all but finitely many primes. Furthermore [5, p. 55], if $M$ is one maximal order and $(N_p)$ is a family of local maximal orders with $M_P = N_P$ for all but finitely many $P$, there is a unique maximal order $N$ having the localizations $N_P$. Hence we can use the results of the previous section to derive a straightforward global classification, though we then have to go on and analyze the group involved. In particular, we shall show that it depends on $S$ much more than on $b$.

Definition. Let $E^1$ be the multiplicative group of elements in $E$ with norm 1. Let $\mathscr{I}^1$ be the group of all families $(x_P)$ where $P$ runs over the primes of $R$, each $x_P$ is in $E^1$, and $x_P$ is a unit of $S_P$ for all but finitely many $P$. Note that $E^1$ is embedded diagonally in $\mathscr{I}^1$. Let $\mathscr{I}_u^1$ be the subgroup of $\mathscr{I}^1$ where each $x_P$ is a unit of $S_P$.

Definition. For each ramified prime $P$, write $PS_P = (\pi)^2$. Let $k$ be the largest integer $\leqslant \mathrm{ord}_\pi(\bar{\pi}-\pi)$ for which there is some $u$ in $E$ with $\mathrm{ord}_\pi(u\bar{u}b-1) \geqslant 2k$. Let $\mathscr{I}^1(b)$ be those elements in $\mathscr{I}_u^1$ such that $x_P$ is congruent to 1 modulo $(\pi)^k$ for each ramified prime.

Theorem 3.1. *The group* $\mathscr{I}^1/\mathscr{I}^1(b)$ *acts simply transitively on the maximal orders in* $A$ *containing* $S$.

*Proof.* We define an action of $\mathscr{I}^1$ on the set of maximal orders as follows. If $M$ is a maximal order and $(x_P)$ is in $\mathscr{I}^1$, then we can apply the

automorphism $\varphi(u+vJ)=u+x_P vJ$ to the localization $M_P$, getting a new local maximal order $N_P$. At all but finitely many primes, the element $x_P$ is a unit and the prime is unramified, so $M_P=N_P$ by (2.6). Thus we can map $M$ to the new maximal order $N$ with these locatizations. Clearly this gives a group action. We know that all maximal orders locally are properly isomorphic, so this action of $\mathscr{I}^1$ is transitive on the set of maximal orders. The computation in (2.6) shows that the stabilizer of any particular $M$ is the subgroup we have called $\mathscr{I}^1(b)$. ∎

COROLLARY 3.2. *The group $\mathscr{I}^1/\mathscr{I}^1(b)\cdot E^1$ acts simply transitively on the proper isomorphism classes of maximal orders containing $S$.*

*Proof.* We just need to observe that the action of $\mathscr{I}^1$ restricted to $E^1$ gives the action of the (global) proper automorphisms. ∎

PROPOSITION 3.3. *The group $\mathscr{I}^1/\mathscr{I}^1(b)\cdot E^1$ is an extension of $\mathscr{I}^1/\mathscr{I}^1_u\cdot E^1$ by a finite abelian group of the form $(\mathbb{Z}/2\mathbb{Z})^m$. Here $m$ is at most the number of ramified primes $(\pi)^2$ for which there exists some $u$ in $E$ with* $\operatorname{ord}_\pi(u\bar{u}b-1)\geqslant 2\operatorname{ord}_\pi(\bar{\pi}-\pi)$.

*Proof.* The extra conditions defining $\mathscr{I}^1(b)$ inside $\mathscr{I}^1_u$ involve only the ramified primes mentioned in the statement; at each such prime they restrict to a subgroup of index 2. Thus $\mathscr{I}^1_u/\mathscr{I}^1(b)$ is the corresponding product of copies of $\mathbb{Z}/2\mathbb{Z}$, and $\mathscr{I}^1_u\cdot E^1/\mathscr{I}^1(b)\cdot E^1$ is a quotient of that product. ∎

The main structure involved in classifying the proper isomorphism classes is thus $\mathscr{I}^1/\mathscr{I}^1_u\cdot E^1$, which depends only on the integral closure $S$ of $R$ in the field extension $E/K$ involved in defining $A$; for many choices of $b$, in fact, we would expect to have $\mathscr{I}^1_u=\mathscr{I}^1(b)$, and then $\mathscr{I}^1/\mathscr{I}^1_u\cdot E^1$ will be exactly the group we want. We now proceed to analyze it in more familiar terms. Recall that an ideal $F$ is called *ambiguous* if $\bar{F}=F$.

THEOREM 3.4. *The following three groups are isomorphic*:

(1) $\mathscr{I}^1/\mathscr{I}^1_u\cdot E^1$

(2) *the (fractional) ideals of $S$ with norm 1 modulo those that are principal with a generator of norm 1,*

(3) *the quotient of the ideal class group of $S$ by the subgroup of classes containing ambiguous ideals.*

*Proof.* The (fractional) ideals in $S$ of norm 1 (i.e., norm $R$) form a free abelian group generated by quotients $\bar{Q}/Q$ for $Q$ lying over split primes $P$. To each element in $\mathscr{I}^1$ we can assign such an ideal, letting the $P$-local

component at each $P$ be $x_P S_P$. This mapping is surjective, since the local generator $\bar{\pi}/\pi$ is in $E^1$, and the kernel is $\mathscr{I}_u^1$. The image of $E^1$ consists of those principal ideals having a generator of norm 1. Thus (1) is isomorphic to (2). But now we can also map ideals onto ideals of norm 1, sending an ideal $F$ to $\bar{F}/F$. We have $\bar{F}/F = xS$ with $Nx = 1$ iff we have $\bar{F}/F = (s/\bar{s})S$ for some $s$; this happens iff $(sF)^- = sF$ for some $s$, which is true iff $F$ is in the same ideal class as an ambiguous ideal. ∎

COROLLARY 3.5. *If $R$ is the ring of integers in a number field, then there are only finitely many proper isomorphism classes of maximal orders containing $S$.*

For $R = \mathbb{Z}$, we can give an even more classical description of our group.

THEOREM 3.6. *Let $R = \mathbb{Z}$. Then $\mathscr{I}^1/\mathscr{I}_u^1 \cdot E^1$ is isomorphic to the principal genus inside the strict ideal class group of $S$.*

*Proof.* We use Theorem 3.4. Recall that by definition two ideals are in the same strict class if their quotient is a principal ideal with a generator of positive norm. Let $C_s$ be the strict ideal class group. It maps onto the ordinary class group $C$. Gauss of course proved that the principal genus is precisely the squares in $C_s$, the image of the homomorphism $[F]_s \to [F^2]_s$. For a principal ideal $fS$, the image is $[f^2 S]_s$, and obviously $N(f^2) = N(f)^2$ is positive, so the homomorphism vanishes on all $fS$ and factors through $C$.

We have $F \cdot \bar{F} = N(F)S$ with $N(F)$ viewed as a positive integer, and so the class of $\bar{F}$ is the inverse of the class of $F$ in $C_s$. Thus a class containing an ambiguous ideal will go to the trivial class when squared. Conversely, let $F$ be an ideal with $F^2 = dS$ for some $d$ of positive norm. We have then $d^{-1}F = F^{-1}$, so $\bar{F} = N(F)\, F^{-1} = N(F)\, d^{-1} F$. As $N(F) = N(\bar{F})$, the element $N(F)\, d^{-1}$ must be a unit, and so its norm is $\pm 1$ in $\mathbb{Z}$. But $N(d) > 0$ by assumption, and so $N(F)\, d^{-1}$ must have norm 1. Writing it as $\bar{c}/c$ for some $c$ in $E$, we get $\bar{c}F$ ambiguous. ∎

## 4. When All Maximal Orders Contain $S$

We shall now show that all maximal orders in our $A$ will contain $S$ unless $b$ satisfies special conditions. This will require a brief review of splitting theory.

Starting with our algebra $A$, we can form an $E$-algebra $A_E = A \otimes_K E$. Inside it as a subalgebra is a copy of $E \otimes_K E \cong E \times E$ on which $J \otimes 1$ satisfies $(J \otimes 1)(u, v) = (v, u)(J \otimes 1)$. Our $E$, the original $K$-algebra, is embedded in it as the elements $x \otimes 1$, which correspond to $(x, \bar{x})$ in $E \times E$.

If we let $e_2$ denote the idempotent $(0, 1)$ in $E \times E$, the set

$$\{1, e_2, e_3 = (1 - e_2)(J \otimes 1), e_4 = e_2((1/\bar{b})J \otimes 1)\}$$

is an $E$-basis of $A_E$. The notation here has been chosen to match the standardized form of basis for such algebras [7]; we have $0 = e_2 e_3 = e_3(1 - e_2) = (1 - e_2)\, e_4 = e_4 e_2$ and $0 = e_3 e_3 = e_4 e_4$. The scaling factor in $e_4$ is introduced to make $e_3 e_4 = 1 - e_2$; the other product $e_4 e_3$ then comes out to be $(1 \otimes \lambda)\, e_2$ where $\lambda = \bar{b}/b$ (If $\lambda$ were exactly 1, we would have the algebra of $2 \times 2$ matrices.)

The maximal $S$-orders in such a "split nonassociative quaternion algebra" have been completely classified by Lee [3]. In particular, we have the following result.

THEOREM A. *Let $Q$ be a prime in $S$. Let $r$ be a nonnegative integer. Then there is a maximal $S_Q$-order in $A_E$ meeting $E \times E$ in $S_Q \cdot 1 + Q^r S_Q \cdot e_2$ if and only if* $\max\{0, \operatorname{ord}_Q(\lambda - 1)\} \geqslant 3r$.

LEMMA 4.1. *Suppose that every maximal $S$-order in $A_E$ contains the copy of $S$ embedded in $E \otimes_K E$ by $s \mapsto s \otimes 1$. Then every maximal order in $A$ contains $S$.*

*Proof.* Suppose $M$ is a maximal $R$-order in $A$. Then $M \otimes_R S$ is an $S$-order in $A_E$. It follows [3] that $M \otimes_R S$ is contained in some maximal $S$-order $\mathcal{M}$. We can view $A$ as a subring of $A_E$ under the embedding $a \mapsto a \otimes 1$. The intersection $\mathcal{M} \cap A$ will be closed under multiplication and be finitely generated over $R$, so it will be an order in $A$. As it contains $M$, it must equal $M$. But by hypothesis it also contains $S$. ∎

THEOREM 4.2. *Let $D$ be the different of $S/R$. Every maximal order of $A$ contains $S$ unless there is some prime $Q$ of $S$ for which* $\operatorname{ord}_Q(\bar{b}/b - 1) \geqslant 3 + 3 \cdot \operatorname{ord}_Q(D)$.

*Proof.* We prove that our condition implies the hypothesis of Lemma 4.1. We will have $S$ contained in a maximal order $\mathcal{M}$ iff it is contained in $\mathcal{M}_P$ for each $P$, and so we can work locally. Suppose first $P$ is inert, so $Q = SP$ is prime. Here of course $\operatorname{ord}_Q(D) = 0$. Obviously our embedded $S$ is contained in $S_Q \times S_Q$, which is contained in $\mathcal{M}_P$ if $r = 0$. If any maximal $S_Q$-order in $A_E$ meets $E \times E$ in something smaller than $S_Q \times S_Q$, then we must have $\operatorname{ord}_Q(\bar{b}/b - 1) \geqslant 3$, by Theorem A. Thus our assertion is true in this case.

Suppose next that $P$ splits, say $PS_P = Q\bar{Q}S_P$. Let $bS_P = Q^m(\bar{Q})^n S_P$. Then $(\bar{b}/b)\, S_P = (\bar{Q}/Q)^{m-n} S_P$. If $m \neq n$, then this is of nonzero order at both $Q$

and $\bar{Q}$, and $\bar{b}/b-1$ has order $\leqslant 0$. Thus only $r=0$ is possible at $Q$ and at $\bar{Q}$, and so $S$ is contained in $\mathcal{M}_P=\mathcal{M}_Q\cap\mathcal{M}_{\bar{Q}}$. When $m=n$, we can have $r\neq 0$, but only when $\bar{b}/b-1$ has order at least 3 at $Q$ or $\bar{Q}$. [In fact, it will have the same order at both, since $\bar{b}/b-1=(-\bar{b}/b)(b/\bar{b}-1)$.]

Finally, suppose $P$ is ramified, so $S_P=S_Q$ with $PS_P=Q^2S_Q$. With the notation of Section 2, we have $\mathrm{ord}_Q(D)=t+1$, and we know [5, p. 69] that every element $s$ in $S_Q$ satisfies $s\equiv\bar{s} \bmod Q^{t+1}S_Q$. We can rewrite $(s,\bar{s})$ in $E\times E$ as $(s,s)+(0,\bar{s}-s)=[1\otimes s]\cdot 1+[1\otimes(\bar{s}-s)]\cdot e_2$. All these elements will therefore be contained in $S_Q\cdot 1+Q^rS_Q\cdot e_2$ so long as $r$ is no greater than $t+1$. Thus there can be a maximal order $\mathcal{M}$ with $\mathcal{M}_Q$ not containing the embedded $S$ only if $\mathrm{ord}_Q(\bar{b}/b-1)\geqslant 3(t+2)$, just as the theorem says. ∎

*Remark.* In the notation of Section 2, a ramified prime $Q$ occurs in $D$ with exponent $t+1$. An arbitrary element of the form $\bar{b}/b-1$ will have $Q$-order $t$ (half the time) or $t+1$ (most of the rest of the time), so the condition in the theorem (order $\geqslant 3t+6$) is quite strict. At unramified primes, of course, a "random" element will not even have $\bar{b}/b-1$ divisible by $Q$, let alone by $Q^3$.

## 5. An Example and Some Questions

We show finally that some hypothesis is indeed necessary in Theorem 4.2. Specifically, we let $R=\mathbb{Z}$, with $S=\mathbb{Z}[\sqrt{2}]$, and we assume that $b$ is in $S$ (not in $R$, of course) and is congruent to 1 modulo a high power of 2. We shall prove that then there are maximal orders in $A$ that do not contain $S$.

First, we know that every order is contained in a maximal order. If we can produce an order that is not contained in any maximal order that contains $S$, then there will have to be other types of maximal orders as well. Looking at the explicit description in (2.5) and observing that our $b$ is certainly a unit at 2, we see that every element $v+wJ$ in a maximal order containing $S$ can have at most the power $(\sqrt{2})^3$ in the denominator of $w$. Thus it will suffice to produce an order containing an element with larger 2-denominator in the $J$-term. As we know that every local maximal order does arise from localization of a global maximal order, it will suffice to produce such an order locally at 2.

Rather than just writing down an example out of nowhere, we sketch a general process for constructing orders in $A$. We start in $A_E$, as in Section 4. Since we have assumed that $b$ is congruent to 1 modulo a high power of 2, we know from Theorem A that there are local maximal orders meeting $E\times E$ in something smaller than $S_{(2)}\times S_{(2)}$. In fact, however, the

construction in [3] gives us such orders explicitly. A typical one is the span of the elements

$$1, \qquad (1 \otimes \sqrt{2})^r e_2, \qquad e_2 + e_3, \qquad (1 \otimes 1/\sqrt{2})^r [1 - 2e_3 - e_3 + e_4].$$

To get a reasonably large denominator in one element, we take $r = 6$. An arbitrary element in this order thus looks like

$$\alpha + (1 \otimes 8\beta)\, e_2 + (1 + \gamma)(e_2 + e_3) + (1 \otimes \delta/8)(1 - 2e_2 - e_3 + e_4)$$

for $\alpha, \beta, \gamma, \delta$ in $S_{(2)}$.

By base extension, $A_E$ has an $E$-basis given by

$$1 \otimes 1, \qquad \sqrt{2} \otimes 1, \qquad J \otimes 1, \qquad \sqrt{2}\, J \otimes 1;$$

this is expressed in terms of the standardized basis by

$$\begin{aligned} \sqrt{2} \otimes 1 &= (1 \otimes \sqrt{2})1 - (1 \otimes 2\sqrt{2})\, e_2 \\ J \otimes 1 &= e_3 + (1 \otimes b)\, e_4 \\ \sqrt{2}\, J \otimes 1 &= (1 \otimes \sqrt{2})\, e_3 - (1 \otimes \sqrt{2}\, b)\, e_4. \end{aligned}$$

Let us rewrite the elements in our $S_{(2)}$-order in terms of the extended basis; then the ones in $A$ will be those with coefficients in $\mathbb{Q}$. That is, each coefficient should be equal to its conjugate. When we write out those conditions, we find that they allow us to solve to get

$$\begin{aligned} \gamma &= (\delta + \bar{\delta}/\bar{b})/8, \\ \beta &= (\bar{\alpha} - \alpha)/8 + (\bar{\delta}/64)(1 - 1/\bar{b}); \end{aligned}$$

the element itself then comes out to be

$$\alpha + \delta/8 + (\bar{\delta}/8\bar{b})J.$$

Thus we have a $\mathbb{Z}_{(2)}$-order in $A$ (not necessarily maximal) consisting of all element of the above form for which $\alpha$ and $\delta$ and also the associated expressions $\gamma$ and $\beta$ are in $S_{(2)}$. So long as $\bar{b} - 1$ is divisible by a high power of 2, the second term in $\beta$ is already in $S_{(2)}$, and $\beta$ will be integral precisely when 8 divides $\bar{\alpha} - \alpha$; this forces $\alpha = m + 4n\sqrt{2}$, with $m$ and $n$ in $\mathbb{Z}_{(2)}$. Rewriting $8\gamma$ as $\delta + \delta - \delta(1 - 1/\bar{b})$, we see similarly that the condition on $\gamma$ requires 8 to divide $(\delta + \delta)$, so $\delta = 4u + v\sqrt{2}$ with $u$ and $v$ in $\mathbb{Z}_{(2)}$. Thus the intersection is the $\mathbb{Z}_{(2)}$-span of

$$1, \qquad 4\sqrt{2}, \qquad (1/2) + (1/2\bar{b})J, \qquad (\sqrt{2}/8) - (\sqrt{2}/8\bar{b})J.$$

Once we have found the example in this way, of course, we can scale the last two elements to eliminate the $\bar{b}$ in the denominator. Direct computation then will show that we get an order for suitable $b$. Here is the explicit statement.

PROPOSITION 5.1. *Let $R = \mathbb{Z}$ with $S = \mathbb{Z}[\sqrt{2}]$, and let $b$ be in $S$ (not in $R$) with $b \equiv 1 \bmod 2^7$. Then the $\mathbb{Z}$-span of the elements*

$$1, \qquad 4\sqrt{2}, \qquad (\bar{b}/2) + (1/2)J, \qquad (\bar{b}\sqrt{2}/8) - (\sqrt{2}/8)J$$

*is an order that is not contained in any maximal order containing $S$. Hence there exist maximal orders not containing $S$.*

Obviously this example raises the problem of classifying all maximal orders in such exceptional cases. The basic questions involved are essentially local:

(1) In the situation of (2.5), the condition of having some $u$ in $E$ with $\operatorname{ord}_\pi(u\bar{u}b - 1) \geqslant 2k$ implies the condition that $\operatorname{ord}_\pi(\bar{b}/b - 1)$ is at least $3k$; but the converse is not true. It seems likely, therefore, that the sufficient condition in Theorem 4.2 is not actually necessary. What are the precise conditions that force all maximal orders to contain $S$?

(2) More generally, starting with $S$ and $b$, how can we determine precisely which $R$-orders inside $S$ occur as intersections of maximal orders with $E$?

(3) If an order $S_0$ occurs as such an intersection, do all orders $S_1$ with $S_0 \subset S_1 \subset S$ also occur? (This is true in the split case.)

(4) Is it true in general that, as in (2.6), all maximal orders having the same intersection with $E$ are locally isomorphic?

We know one possible line of attack on these questions. The analysis in (4.1) shows that all maximal orders of $A$ are intersections of $A$ with the maximal orders of $A_E$. All maximal orders of $A_E$ are described in [3], and locally the description gives explicit bases. The method of (5.1) then gives an explicit computation of the intersections. The problem is that almost all of these intersections are not actually maximal orders, and as yet we have not found a reasonable analysis of the inclusions among them.

## REFERENCES

1. N. BOURBAKI, "Algèbre Commutative," Chap. 5, Entiers, Hermann, Paris, 1964.
2. L. E. DICKSON, Linear algebras with associativity not assumed, *Duke Math. J* **1** (1935), 113–125.

3. H. J. LEE, Maximal orders in split nonassociative quaternion algebras, *J. Algebra* **146** (1992), 427–440.
4. I. REINER, "Maximal Orders," Academic Press, New York, 1975.
5. J.-P. SERRE, "Corps Locaux," Hermann, Paris, 1962.
6. M.-F. VIGNERAS, "Arithmétique des algèbres de quaternions," Lecture Notes in Math., Vol. 800, Springer, New York, 1980.
7. W. C. WATERHOUSE, Nonassociative quaternion algebras, *Algebras Groups Geom.* **4** (1987), 365–378.